SOFTMAIL®

เอ็นคริพชัน

การป้องกันข้อมูลที่เป็นความลับ จากการเก็บในฮาร์ดดิสค์หรือสื่อสารข้อมูล

ยืน ภู่วรวรรณ

ฮาร์ดดิสค์ เป็นแหล่งเก็บข้อมูลที่มีความสำคัญเพิ่มขึ้น ฮาร์ดดิสค์เป็นแหล่งที่อยู่ของข้อมูลจำนวนมาก และที่สำคัญคือ อาจจะมีข้อมูลหลายประเภทอยู่ร่วมกัน และมีผู้ใช้คอมพิวเตอร์ร่วมกันหลายคน การป้องกันความลับจากการเก็บข้อมูลไว้ในฮาร์ดดิสค์เดียวกันนั้น จึงเป็นเรื่องที่พูดถึงกันบ่อยมากขึ้น เมื่อเป็นเช่นนี้ ผู้เขียนก็มาคิดดูว่าน่าจะมีวิธีใดบ้างที่จะป้องกันข้อมูลได้ ผู้เขียนก็เสนอไปหลายวิธีแล้ว เช่น การสร้างรหัสผ่าน การแบคอัพข้อมูลส่วนตัวแล้วลบในส่วนฮาร์ดดิสค์ทิ้งไป อย่างไรก็ตาม วิธีหนึ่งที่ผู้เขียนยังไม่กล่าวถึงและอยากจะกล่าวถึงในที่นี้คือวิธีการ **"เอ็นคริพชัน"**

หลักการของเอ็นคริพชันหรือการป้องกันการอ่านข้อมูลให้เข้าใจได้เป็นเรื่องที่มีมานานแล้ว ตามหลักฐานทางประวัติศาสตร์มีมาแล้วกว่า 2,000 ปี หลักและวิธีการเอ็นคริพมีมากมาย โดยเฉพาะเมื่อนำข้อมูลมาใช้กับคอมพิวเตอร์ วิธีการของการสร้างการเอ็นคริพชันข้อมูลก็ได้พัฒนาไปอีกมาก เพราะการใช้โปรแกรมคอมพิวเตอร์ช่วยถอดรหัสเป็นไปได้ง่ายขึ้น การสร้างรหัสเอ็นคริพชันในระยะหลังจึงต้องใช้แฟกเตอร์แปรอีกหลายอย่างมาประกอบด้วย เช่นเวลา จึงทำให้รหัสเอ็นคริพชันแปรเปลี่ยนไปตามเวลา

สำหรับมุมดีเบสฉบับนี้ ได้พยายามจัดเรื่องให้เหมาะสมกับหัวข้อหลักของเล่มจึงนำเอาเรื่องของเอ็นคริพมาประยุกต์ให้ผู้สนใจได้เข้าใจหลักวิธีการและหาทางประยุกต์ไปใช้ต่อไป

หลักและวิธีของการเอ็นคริพชันเบื้องต้น

วิธีการที่ใช้กันมาแบบพื้นฐานและเป็นที่รู้จักกันมานานแล้ว มีสองหลักการคือ แบบแทนที่ (substitution) และแบบสลับเคลื่อนย้ายตำแหน่ง (transposition) หลักการแบบการแทนที่เป็นการแทนตัวอักษรหนึ่งด้วยอักษรอีกตัวหนึ่ง แต่ต้องรู้สูตรหรือค่าว่า ตัวอักษรแต่ละตัวแทนค่าอะไรไว้ เพื่อจะได้ทำการถอดรหัสกลับคืนมาได้ ส่วนแบบสลับตำแหน่งเป็นแบบที่เราให้ตัวอักษรในข้อความสลับที่อยู่กัน

อย่างไรก็ตาม ยังมีวิธีการเอ็นคริพชันได้อีกหลายวิธี โดยเฉพาะเมื่อใช้กับคอมพิวเตอร์ เช่นการสลับบิต หรือการจัดการกำหนดบิตต่างๆของข้อมูลให้แตกต่างกันออกไป

วิธีการเอ็นคริพชันทุกวิธีจะต้องมีคีย์ในการกำหนดวิธีการ คีย์ในที่นี้ก็หมายถึง กลุ่มตัวอักษรที่เป็นตัวกำหนดรหัสหรือถอดรหัส คีย์ที่กำหนดนี้จะรู้ได้เฉพาะเจ้าตัวเท่านั้น การกำหนดคีย์จึงต้องถือเป็นความลับ

ลองพิจารณาวิธีการใช้งานในการทำเอ็นคริพชันข้อมูลดูวิธีแรก ซึ่งเป็นการสร้างรหัสแทนค่าอย่างง่าย

ตัวอย่างที่กล่าวถึงนี้เป็นการเอาค่าคงที่โดยการออฟเซ็ต เช่น รหัสตัวอักษรต่อไปนี้

abcdefghijklmnopqrstuvwxyz

เมื่อออฟเซ็ตค่าด้วย 3 จะเป็น

defghijklmnopqrstuvwxyzabc

สังเกตว่า a ของข้อมูลจะถูกเอ็นคริพเป็นรหัส d b จะเป็น e ดังนั้นข้อความ

meet me at sunset

จะกลายเป็น

phhw ph dw vxqvhw

และเพื่อให้การออฟเซ็ตมีค่าแปรเปลี่ยนไปได้อีกตามการตั้งรหัสเพื่อสร้างรหัส (code) หรือการถอดรหัส (decode)

ตัวอย่างของโปรแกรมที่เขียนนี้จะให้ผู้ใช้สร้างคีย์ออฟเซ็ตของตัวเอง เหมือนเป็นรหัสผ่านของการกำหนดออฟเซ็ต ดังนั้นการถอดรหัสก็จะต้องใช้ออฟเซ็ตตรงกันจึงจะได้ผล ลองดูโปรแกรมที่ 1

โปรแกรมที่เขียนเริ่มต้นด้วยการถามว่าจะให้ทำการเอ็นคริพแฟ้มข้อมูลชื่ออะไร ผู้ใช้ต้องกรอกข้อมูลส่วนนี้ เมื่อกรอกชื่อแฟ้มแล้วโปรแกรมจะนำมาตรวจสอบว่ามีอยู่ในดิสค์หรือไม่ ถ้าไม่มีก็จะบอกให้รู้ว่า *'No file'* แล้วให้ป้อนชื่อไฟล์ แต่ถ้ามีโปรแกรมจะผ่าน if ในลูปแรกมายัง else

สังเกตโปรแกรมจะ use & mfile คือใช้แฟ้มข้อมูล แล้ว copy ไปไว้ยังชื่อ tstru แบบ extended เพื่อให้ข้อมูล

ของชื่อฟิลด์ ชนิดฟิลด์ ความกว้างฟิลด์ ไปเป็นข้อมูลของ tstru.dbf

โปรแกรมจะถามว่า D คือ การ decode หรือ C คือการ code ถ้าตอบ C ก็จะให้กรอก key แบบ 5 ตัวอักษร

โปรแกรมจะนำค่าของตัวอักษรทั้ง 5 มาบวกกันแล้ว MOD กับ 10 เอาเศษมาเป็นออฟเซ็ต ดังนั้นค่าของออฟเซ็ตจึงเป็นได้ตั้งแต่ 0-9 แต่ถ้า xvalue หรือค่าออฟเซ็ตเป็น 9 เราจะเปลี่ยนเป็น 10 เพราะค่า 0 ไม่มีประโยชน์

ส่วนโปรแกรมการ code หรือสร้างเอ็นคริพชันนั้น เป็นการอ่านข้อมูลมาดูทีละฟิลด์ ถ้าฟิลด์ใดเป็นตัวอักษร เราจะเอ็นคริพด้วยค่าออฟเซ็ต ถ้าเป็นตัวเลขก็จะไม่มีการเปลี่ยนแปลง

สังเกตการใช้ชื่อ field_type, field_len และ field_name ซึ่งทำให้เรารู้ค่าโครงสร้างโดยละเอียดของแฟ้มข้อมูลได้ โดยดูจาก tstru ซึ่งมาจาก copy แบบ extended

การดีโค้ดก็เช่นเดียวกัน โดยการนำข้อมูลในฟิลด์ที่เป็นตัวอักษรมาแก้ไข โดยเปลี่ยนเป็นค่าใหม่โดยลบออฟเซ็ตออก

ตัวอย่างดังกล่าวทำงานได้ดังรูปที่ 1

เพิ่มแบบการเอ็นคริพให้ยากขึ้น

การใช้วิธีการออฟเซ็ตเป็นเรื่องที่ผู้อ่านข้อมูลอาจเดาใจได้ และง่ายต่อการค้นหาคีย์เพื่อถอดรหัส ทางแก้วิธีหนึ่งให้ผู้ค้นหายากขึ้น คือการแทนที่แบบหนึ่งต่อหนึ่ง คือตัวอักษรหนึ่งจะใช้ตัวอักษรอีกตัวหนึ่งแทนที่ ดังเช่น

ข้อความต้นแบบ

abcdefghijklmnopqrstuvwxyz <space>

เราแทนคีย์เป็น

qazwsxedcrfvtgbyhnujm ikolp

โปรแกรมที่ 1
Encription code & decode

```
*Program : Encription Code and decode
*Author name : Poovarawan
*dBASE Cornor Micro 35
*
clear
set talk off
set stat off
set safety off
clear all
more='Y'
do while upper(more)='Y'
 @ 5,30 say 'Encription by dbase programming'
 @ 8,1 to 8,78
 mfile=space(8)
 @ 15,20 say 'Enter file to Encript (code or decode) :' get mfile
 read
 mvar=trim(mfile)+'.dbf'
 if .not. file('&mvar')
  @ 9,0 clear
  @ 15,10 say 'No file'
  wait
  loop
 else
  @ 9,0 clear
  use &mfile
  copy to tstru stru extended
  sele 2
  use tstru
  sele 1
 endif
 ans=space(1)
 @ 10,10 say 'Which type... (C)ode or (D)ecode ' get ans
 read
 if upper(ans)='C'
  @ 5,0 clear
  key=space(5)
  @ 10,10 say 'Enter your key :' get key
  read
  @ 20,10 say 'Please wait...
  p=asc(left(key,1))+asc(substr(key,2,1))+asc(substr(key,3,1))
  q=asc(substr(key,4,1))+asc(substr(key,5,1))
  xvalue=mod(p+q,10)
  if xvalue=0
   xvalue=10
  endif
  sele 1
  go top
  do while .not. eof()
   sele 2
   go top
   do while .not. eof()
    if field_type ='C'
     m=1
     mdata=''
     do while m<=field_len
      f=field_name
```

โปรแกรมที่ 1 (ต่อ)

```
      y=asc(substr(a->&f,m,1))+xvalue
      if y>127
       y=mod(y,127)+32
      endif
      mdata=mdata+chr(y)
      m=m+1
     enddo
    endif
    sele 1
    repl &f with mdata
    sele 2
    skip
   enddo
   sele 1
   skip
  enddo
  more='n'
 endif
 if upper(ans)='D'
  @ 5,0 clear
  key=space(5)
  @ 10,10 say 'Enter your key :' get key
  read
  @ 20,10 say 'Please wait...'
  xvalue=mod(asc(left(key,1))+asc(substr(key,2,1))+asc(substr(key,3,1))+asc(substr(key,4,1))+asc(substr(key,5,1)),10)
  sele 1
  go top
  do while .not. eof()
   sele 2
   go top
   do while .not. eof()
    if field_type ='C'
     m=1
     mdata=''
     do while m<=field_len
      f=field_name
      y=asc(substr(a->&f,m,1))-xvalue
      if y<32
       y=127-(32-y)
      endif
      mdata=mdata+chr(y)
      m=m+1
     enddo
    endif
    sele 1
    repl &f with mdata
    sele 2
    skip
   enddo
   sele 1
   skip
  enddo
  more='n'
 endif
enddo
return
```

ในที่นี้คือให้ a แทนด้วย q b แทนด้วย a... การกำหนดคีย์แบบนี้ให้ข้อดีคือ เรามีรูปแบบคีย์ได้ถึง n! เช่น ถ้ามีตัวอักษร 26 ตัวก็ได้ 26! รูปแบบนับว่ามีขนาดใหญ่มาก

จากวิธีดังกล่าว ข้อความ meet me at sunset จะกลายเป็น tssjptspqj pumqusj

ก็ยังไม่ยากเกินกว่าจะหาคีย์

การแทนค่าแบบหนึ่งต่อหนึ่งนั้น ถึงแม้จะได้ความเป็นไปได้ถึง n! แต่ก็มีวิธีการหาคีย์ได้ว่าตัวอักษรใดแทนตัวอักษรใด วิธีการหาก็ด้วยการนำข้อมูลทั้งหมดมาเข้าเครื่องคอมพิวเตอร์แล้ววิเคราะห์หาความถี่ เพราะความถี่ของตัวอักษรมีช่วงการแจกแจงที่หาได้อยู่แล้ว เช่น ความถี่ของตัวภาษาอังกฤษจะเป็นดังรูปที่ 2 และความถี่สำหรับตัวอักษรไทยจะเป็นดังรูปที่ 3

จากความถี่นี้เองถ้าผู้วิเคราะห์นำข้อมูลมาแจกแจงความถี่แล้วเปรียบเทียบกับตารางก็จะพอถอดคีย์ออก วิธีนี้จึงเป็นวิธีที่ถอดคีย์ได้อีกเช่นกัน

เพิ่มคีย์ซ้อนมากกว่า 1 คีย์

เพื่อหลีกเลี่ยงปัญหาการถอดคีย์โดยการเปรียบเทียบความถี่ที่ใช้ จึงต้องใช้คีย์มากกว่า 1 คีย์ เช่น

ข้อความเดิม

abcdefghijklmnopqrstuvwxyz<*space*>

คีย์ 1

qazwsxedcrfvtgbyhnujm<*space*>ikolp

คีย์ 2

poi<*space*>uytrewqasdfghjklmnbvcxz

จะเห็นว่า a อาจเป็น q หรือ p ก็ได้ หรือ b อาจเป็น a หรือ o... การที่มีคีย์สองคีย์จะทำให้ถอดคีย์โดยใช้ค่าความถี่ทำได้ยากขึ้น วิธีการใช้คีย์สองคีย์นี้ต้องตั้งกฎเกณฑ์บางอย่างเพิ่มขึ้น เช่น

```
. use sample
. list
Record#  F1                                F2 F3
      1  abcdefghijklmnopqrstuvwxy      123 z{¦}~ !@#$
      2  !!!!!!!!!!fadskhjfgdasjkh        3 hjlgdsgsdj
      3  hjlhgdsjlhgdsjlhdgsfjhdsf        4 sdjhgsdjkj
```

แฟ้มข้อมูลต้นฉบับ

```
.
. list
Record#  F1                                F2 F3
      1  fghijklmnopqrstuvwxyz{¦}~      123!"#$%&E()
      2  &&&&&&&&&&kfixpmoklifxopm        3 moqlixlxio
      3  moqmlixoqmlixoqmilxkomixk        4 xiomlxiopo
```

เมื่อผ่านการใส่รหัสเอ็นคริพแล้วผลจะเป็นดังนี้

รูปที่ 1

a จะแทนด้วย q แต่ถ้าแทนไป 2 ครั้งแล้ว จะแทนด้วย p อีกสองครั้งสลับกันไป ดังนั้นโปรแกรมการเอ็นคริพจะเปลี่ยนค่าโดยนับครั้งด้วยและแทนค่าด้วยคีย์ใดคีย์หนึ่งตามเงื่อนไข จะเห็นว่าวิธีนี้จะยากต่อการถอดคีย์มากขึ้น

การสลับตำแหน่งตัวอักษร

อีกวิธีหนึ่งของการเอ็นคริพที่ทำมาแต่โบราณแล้วคือการสลับตำแหน่ง เพื่อให้ง่ายเข้าจะขอยกตัวอย่างประกอบดังนี้

เอกสารที่ส่ง meet me at sunset เราจะเอามาจัดเข้าอะเรย์เป็น

	m	e	e	t		
	m	e		a	t	
		s	u	n	s	
	e	t	o	o	o	
	o	o	o	o	o	

ข้อความดังกล่าวนี้ เมื่อส่งไปจะดูทางคอลัมน์แทนทางแถว ผลจะได้เป็น mm e..eest...e u...tan.. ts... ข้อความดังกล่าวจะอ่านได้ยากขึ้น

A	2525	I	2242	Q	62	Y	356
B	532	J	39	R	1656	Z	20
C	838	K	94	S	1672	space	5710
D	1145	L	1103	T	3082	Period	234
E	3326	M	1140	U	869	Comma	513
F	828	N	2164	V	376		
G	529	O	1767	W	370		
H	1086	P	697	X	178		

รูปที่ 2 ความถี่ของตัวอักษรภาษาอังกฤษ

ตัวอักษร	ค่าความถี่	เปอร์เซ็นต์ความถี่
	670	0.1446
ก	19963	4.3092
ข	5599	1.2086
ค	8332	1.7985
ฆ	111	0.0240
ง	19176	4.1393
จ	7259	1.5669
ฉ	519	0.1120
ช	4366	0.9424
ซ	1049	0.2264
ฌ	1	0.0002
ญ	1239	0.2674
ฎ	98	0.0212
ฏ	210	0.0453
ฐ	465	0.1004
ฑ	50	0.0108
ฒ	167	0.0360
ณ	1663	0.3590
ด	10813	2.3341
ต	8407	1.8147
ถ	2386	0.5150
ท	11004	2.3753
ธ	1361	0.2938
น	28917	6.2420
บ	7892	1.7036
ป	8266	1.7843
ผ	2272	0.4904
ฝ	317	0.0684
พ	5548	1.1976
ฟ	505	0.1090
ภ	1101	0.2377
ม	16406	3.5414
ย	13854	2.9905
ร	22720	4.9043

ตัวอักษร	ค่าความถี่	เปอร์เซ็นต์ความถี่
ฤ	162	0.0850
ล	10365	2.2374
ว	12882	2.7807
ศ	1615	0.3486
ษ	1139	0.2459
ส	8511	1.8372
ห	9802	2.1158
ฬ	63	0.0136
อ	20346	4.3919
ฮ	120	0.0259
ะ	8765	1.8920
า	32908	7.1035
ำ	3658	0.7896
เ	18084	3.9036
แ	6846	0.4773
โ	2321	0.5010
ใ	5346	1.1540
ไ	7068	1.5257
ๆ	825	0.1781
ฯ	89	0.0192
็	4180	0.9023
่	3993	0.8691
้	8887	1.9183
๊	12388	2.6741
๋	2650	0.5720
์	5443	1.1749
๐	13129	2.8340
๑	4848	1.0465
๒	22600	4.8784
๓	16684	8.6014
๔	165	0.0356
๕	159	0.0343
๖	2567	0.5541
๗	1953	0.4216

รูปที่ 3 ความถี่ของตัวอักษรภาษาไทย

ส่งท้าย

วิธีการเอ็นคริพชันที่ยกมาให้ดูด้วยดีเบสนี้ เป็นเพียงตัวอย่างการประยุกต์อย่างง่าย โดยใช้ออฟเซ็ต สำหรับวิธีการอื่นก็ทำได้โดยโปรแกรมดีเบสเช่นกัน อย่างไรก็ตามเมื่อผู้เขียนได้ลองเขียนโปรแกรมดู พบว่าการแปลงข้อมูลขนาดใหญ่จะใช้เวลามาก ดังนั้นหากต้องการนำโปรแกรมนี้ไปใช้ ผู้เขียนแนะนำให้ใช้คลิปเปอร์คอมพายล์โปรแกรมเสียก่อน

เอกสารอ้างอิง

1. Herbert Schildt, "Advance C", Osborn Mc Grawhill, Berkeley, California.

โฆษณา ย่อย ฟรี

คอลัมน์นี้เปิดโฆษณาฟรี
สำหรับ**ทุกท่านที่ต้องการซื้อขาย**
หรือแลกเปลี่ยนอุปกรณ์
ที่เกี่ยวกับไมโครคอมพิวเตอร์ทุกชนิด
โดย**ไม่เกี่ยวข้องในเชิงการค้า**แต่อย่างใด
และไม่เกี่ยวข้องผูกพันกับบริษัท
หรือห้างร้านที่ทำการค้าด้วย
ข้อความที่จะส่งมาให้พิมพ์ดีด
หรือเขียนตัวบรรจงไม่เกิน 250 ตัวอักษร
ซึ่งรวมถึงชื่อที่อยู่ที่ชัดเจนด้วย

◆

ขายแมคอินทอช รุ่น 512K มี external drive 1 ตัว ดิสค์โปรแกรม 3.5 นิ้ว 30 แผ่น พร้อมคู่มือ 7 เล่ม (ซื้อจาก บ.สหวิริยาฯ)
ราคา 65,000 บาท
ติดต่อ ธรรมสถิตย์ ลิ้มติยะกุล
273/11-13 ถ.มะลิวัลย์ อ.ชุมแพ
ขอนแก่น โทร. 043-311180

◆◆

ขายอุปกรณ์แอปเปิ้ล PAL card, ไดรฟ์ 1 ตัว, มอนิเตอร์, Z80 การ์ด, คอนโทรลเลอร์การ์ด, 80 คอลัมน์+ไทย, คีย์บอร์ดแยก ราคาถูก
ขายจอยสติ๊ก ใช้กับไอบีเอ็ม
ราคา 400 บาท
ติดต่อ คชเดช โทร. 5853847
หลัง 19.00 น.

◆◆◆

กรุณาส่งข้อความโฆษณาถึง
"โฆษณาย่อยฟรี"
วารสารไมโครคอมพิวเตอร์
เลขที่ 800/43-45 ซอยตระกูลสุข
ถ.อโศก-ดินแดง ห้วยขวาง กท. 10400
วารสารไมโครคอมพิวเตอร์สงวนสิทธิ์
ที่จะนำลงหรือคัดออกข้อความใด ๆ
ก็ได้ตามที่เห็นสมควร